MATEMATIK
Chalmers tekniska högskola

Tentamen i TILLÄMPADE DISKRETA STRUKTURER
07 mars 1998, kl 8.45–12.45

Hjälpmedel: Valfri miniräknare, men inga egna anteckningar.
Telefonvakt: Frederik Abrahamsson, 772 5331

OBS! Linje och inskrivningsår samt namn och personnummer skall anges.

---

1. Betrakta RSA-kryptot med $n = 3 \cdot 11 = 33$ och krypteringsnycklen $e = 3$. Vi koderar A–Ö som 1–28, mellanslag som 29, @=30, $=31, &=32 och punkt som 0.
a) Kryptera ordet 'TENTAMEN'.
b) Bestäm dekrypteringsnyckeln d och dekryptera 'L@ÄKABNCLL'.

2. a) Visa att ett element $a \in \mathbb{Z}_n$ har en invers om och endast om $SGD(a, n) = 1$.
b) Motivera att ringen $\mathbb{Z}_n$ är en kropp om och endast om n är ett primtal.

3. Enligt Kinesiska restsatsen är $f \colon \mathbb{Z}_{1221} \to \mathbb{Z}_{33} \times \mathbb{Z}_{37}$, $n \mapsto (n \bmod 33, n \bmod 37)$ en isomorfism. Ange inversen f^{-1} explicit och beräkna $f^{-1}(10, 20)$.

4. Bestäm den disjunktiva normalformen för den booleska funktionen

$$f(x, y, z) = \overline{x}y + \overline{y(x + z)}\,.$$

Ange också den disjunktiva normalformen för $\overline{f}$.

5. Visa att polynomet $p(X) = X^5 + X^3 + X^2 + X + 1$ är primitivt i $\mathbb{Z}_2[X]$. Använd detta för att konstruera kodningspolynomet för en BCH-kod med vikt minst 5.

6. Bestäm det minsta linjärt återkopplade skiftregistret som genererar den periodiska sekvensen $s = (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, \ldots)$ över $\mathbb{Z}_2$.

7. Låt $GL(2, \mathbb{Z}_2)$ vara mängden av alla 2×2 matriser A med element i $\mathbb{Z}_2$ och med determinant $\det A \neq 0$. Visa att $GL(2, \mathbb{Z}_2)$ är en grupp med avseende på matrismultiplikation. Bestäm ordningen av alla element. Ange alla delgrupper. Med vilken känd ändlig grupp är $GL(2, \mathbb{Z}_2)$ isomorf?

8. Visa att $\omega = 2$ är en primitiv åttonde enhetsrot i $\mathbb{Z}_{17}$ med $\omega^4 = -1$ och använd snabb Fouriertransform baserad på ω för att beräkna

$$(1 + X + 3X^2 + 3X^3)(1 + 3X^2 + X^3)$$

i $\mathbb{Z}_{17}[X]$. Använd resultatet för att beräkna $245 \cdot 113$ (eller hexadecimalt: `F5` $\cdot$ `71`).
(8 p)